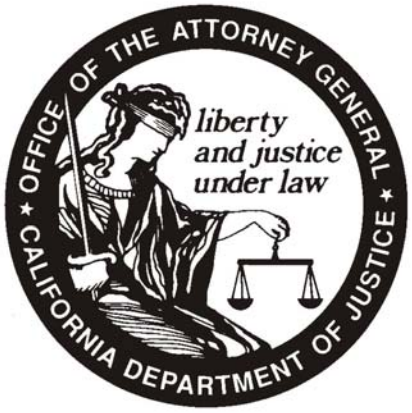
Electronic Recording Delivery System

Vendor of Software Certification Handbook



DRAFT

VERSION 1

California Department of Justice
CJIS Operations Support Bureau
Electronic Recording Delivery System Program

ELECTRONIC RECORDING DELIVER SYSTEM (ERDS)
VENDOR OF SOFWARE CERTIFICATION HANDBOOK
TABLE OF CONTENTS

SECTION 11 Escrow Requirements

SECTION 12 Security Audit Requirements

SECTION 13 Appendices

Terms and Conditions - Vendor
Social Security Number Privacy Statement
Fee Schedule - PENDING
Disqualifying Offenses
Statutory Authority, Chapter 621
Statutory Authority, Chapter 520
Regulations – PENDING
Baseline Requirements and Technology Standards
Forms:
ERDS 0003 - Application for Vendor of Software Certification
ERDS 0005 - Application Attachment Vendor Employee(s) and/or Business Entity(ies), Attachment A
ERDS 0009 - Vendor Application Form for Reference(s), Attachment B
ERDS 0006 - Request for Replacement of Certificate or Application Documents
ERDS 0010 - Application for Withdrawal

(Fingerprinting Requirements Document)
BCII 9004 - Request for Exemption from Mandatory Electronic Fingerprint Submission Requirement
BCII 8016 - Sample Request for Live Scan Service
FD 258 - Fingerprint Hard Card

SECTION 1
INTRODUCTION

The Electronic Recording Delivery Act of 2004 authorizes a County Recorder, upon approval by resolution of the board of supervisors and system certification by the Attorney General, to establish an Electronic Recording Delivery System (ERDS) for the delivery and recording of specified digitized or digital electronic records that are an instrument of real estate transactions, subject to specified conditions, including system certification, regulation, and oversight by the Attorney General (Government Code section 27390-et seq).

Individuals requesting certification as a Vendor of Software and/or for the approval of software must contact the ERDS program and request the Vendor of Software Certification Package. ERDS staff will inform the applicant of the availability of the Vendor of Software Certification Package on the AG's website, http://ag.ca.gov/ or will, at the request of the applicant, send the package via ground mail.

Within the Attorney General's office, the ERDS Program, within the Department of Justice, has been established and is responsible for implementing the requirements of the law.

ERDS Program contact information:

Department of Justice
Electronic Recording Delivery System Program
P.O. Box 160526
Sacramento, CA 95816-0526

Telephone:	(916) 227-8907
Fax:	(916) 227-0595
E-mail address:	erds@doj.ca.gov
Website:	http://caag.ca.gov/erds

The following procedures establish the requirements to be met for the certification of vendors offering software to County Recorders for electronic recording delivery systems.

It is important to understand that the Certification of a Vendor of Software does not automatically approve their software. In order to obtain approval of software, a Vendor of Software must read Section C of the ERDS 0003, Application for Vendor of Software Certification, and certify and sign, under penalty of perjury, that the software meets the Baseline Requirements and Technology Standards established by the Attorney General. The approval of the software certificate will include a "disclaimer" stating that the software is not being approved as to its ability to service/function in an ERDS operational environment nor that it meets all County Recorder's requirements; only that the vendor

has stated that it meets the Department of Justice Baseline Requirements and Technology Standards as of the date of the Attorney General's software approval.

SECTION 2
DEFINITIONS

For a detailed explanation of the Definitions used throughout the process of establishing an Electronic Recording Delivery System, refer to the Baseline Requirements and Technology Standards information found in Section 13 – Appendices.

SECTION 3
CONTENTS OF VENDOR OF SOFTWARE CERTIFICATION PACKAGE

The Vendor of Software Certification Package will contain the following material:

1. ERDS 0003, Application for Vendor of Software Certification, ERDS 0005, Application Attachment Vendor Employee(s) and/or Business Entity(ies) Attachment A, and, ERDS 0009, Vendor Application Form for Reference(s), Attachment B.
2. BCII 8016, Request for Live Scan Service – Preprinted with the ERDS Originating Agency Identifier (ORI) address, mail code, and level of service (for use when submitting fingerprints using the Live Scan Method).
3. FD 258, Fingerprint Hard Card – for use when submitting fingerprints using the Manual Hard Card Method.
4. BCII 9004, Request for Exemption from Mandatory Electronic Fingerprint Submission Requirement must accompany a FD 258, Fingerprint Hard Card. NOTE: Where Live Scan locations are available, hard card submission will not be accepted.
5. Vendor of Software Certification Handbook containing the following information:

    - Definitions – Refer to Section 13 Appendices – Baseline Requirements and Technology Standards, Pages 3-14
    - Vendor of Software Criteria
    - Escrow Requirements
    - Security Audit Requirements
    - Terms and Conditions – Vendor
    - Social Security Number Privacy Statement
    - Fee Schedule – PENDING
    - Disqualifying Offenses
    - Statutory Authority – Chapter 621
    - Statutory Authority – Chapter 520
    - Program Regulations - PENDING
    - Baseline Requirements and Technology Standards
    - Forms

SECTION 4
CERTIFICATION REQUIREMENTS OF A VENDOR OF SOFTWARE

Individuals proceeding with the Vendor of Software Certification process must comply with the following:

1. Submit a completed ERDS 0003, Vendor of Software Certification and ERDS 0005, Application Attachment Vendor Employee (s) and/or Business Entity(ies) and ERDS 0009, Vendor Application Form for Reference(s) Attachment B if applicable, to the address on the application. This application must be dated and signed under penalty of perjury attesting to the fact that the applicant has read the materials contained in the Vendor of Software Certification Package. A signed application will indicate that the applicant understands and agrees to the disclaimer addressing the Approval of Software and the established Terms and Conditions – Vendor.
2. Vendor shall submit the Letter of Deposit as outlined in the Escrow Requirements to the County Recorder.
3. Submit a check or money order, no cash, for all fees. Fees are non-refundable (refer to Fee Schedule).
4. Submit additional Vendor of Software criteria as outlined in Section 5 of this handbook.
5. Submit a signed Social Security Number Privacy Statement.
6. Submission of fingerprints by one of the following methods:

NOTE: ***Beginning July 1, 2005 all applicant fingerprint submissions must be transmitted electronically (Follow Step a). In some rare circumstances, fingerprint Hard Cards will be accepted if an applicant provides the Department of Justice with a valid reason for not submitting by Live Scan and the Department of Justice waives the requirement of electronic submission. In those instances, the BCII 9004, Request for Exemption From Mandatory Electronic Fingerprint Submission Requirement shall be submitted (Follow Step b).***

a. Submitting Fingerprints via Live Scan (Electronic Submission) services may be obtained at most law enforcement agencies. To obtain the most current locations where live scan fingerprint services are available, an applicant may go on-line to the Attorney General's home page or the Applicant Fingerprint Submission page, both found at http://caag.state.ca.us.

The BCII 8016, Request for Live Scan Service must be submitted to the law enforcement and/or other agency providing the live scan services. Applicants are encouraged to access the fingerprint web site, www.caag.state.ca.us/fingerprints for fingerprinting locations in their area and to determine if an appointment for fingerprinting is required, if

additional fees may be charged for the fingerprint rolling services, and the acceptable method of payment. Fingerprinting fees totaling $57.00 ($32.00 for the state fingerprint submissions and $24.00 for the federal fingerprint submission) will be required. Amounts do not include separate fees that may be charged by an agency for rolling fingerprints

After the live scan services are performed, the applicant will receive a copy of the BCII 8016, Request for Live Scan Service. Submit ERDS 0003, Application for Vendor of Software Certification along with the copy of the BCII 8016, Request for Live Scan Service, as proof of fingerprinting.

b. Fingerprints Submitted via FD 258, Fingerprint Hard Card (Manual Submission) maybe submitted, if fingerprinting has been provided by a certified fingerprint roller. The individual needs to submit their FD 258, Fingerprint Hard Card along with the ERDS 0003 Application for Vendor of Software Certification. The fingerprint card **must** include the certified fingerprint roller's signature and certification number next to their signature. If the quality of the fingerprint image is poor, if data fields are not properly completed, or the signature and certification number of the fingerprint roller are missing, the applicant fingerprint card will be rejected and returned to the applicant.

   In addition, the FD-258, Fingerprint Hard Card must be accompanied by a BCII 9004, Request for Exemption From Mandatory Electronic Fingerprint Submission Requirement. Fingerprinting fees totaling $57.00 ($32.00 for the state fingerprint submissions and $24.00 for the federal fingerprint submission) are required. A **separate** check or money order made payable to the "California Department of Justice-ERDS Program" must accompany ERDS 0003, Application for Vendor of Software Certification and separate sets of fees must be mailed to the Department of Justice at the address indicated on the application.

c. Individuals residing outside of California and applying for certification in California who cannot be fingerprinted in California must have their fingerprints rolled at a law enforcement agency in their state of residence. A fingerprint-rolling fee may be collected by the law enforcement agency when fingerprints are taken.

   If living outside of California, fingerprints must be submitted via FD 258, Fingerprint Hard Card with the ERDS 0003, Application for Vendor of Software Certification. Fingerprint processing fees totaling $57.00 ($32.00 for the state fingerprint submission and $24.00 for the federal fingerprint submission) are required. A **separate** check or money order made payable to the "California Department of Justice-ERDS Program" must accompany the ERDS 0003, Application for Vendor of Software

Certification. The application, fingerprints, and processing fees must be mailed to the Department of Justice at the address indicated on the application.

SECTION 5
VENDOR OF SOFTWARE CRITERIA

A vendor may apply as an individual or as a company. When applying as a company, the vendor must provide a list identifying those employees and/or business entities employed by or contracted with the vendor whom will be utilized in the development, installation, testing, and maintenance of an ERDS. Refer to ERDS 0005, Application Attachment Vendor Employee(s) and/or Business Entity(ies). Employees and/or business entities serving in this capacity shall be subject to the fingerprint background requirements prior to approval of a vendor certification.

An individual seeking certification as a vendor may apply for software approval on the same application, as outlined in Step 5 below.

The ERDS program will respond to the vendor with an approval or denial within an estimated timeframe of 90 days of receipt of the application and all associated documents.

The Certification of a Vendor of Software will be based on the following criteria:

1. Receipt of completed ERDS 0003, Application for Vendor of Software Certification, including ERDS 0005, Application Attachment Vendor Employee(s) and/or Business Entity(ies) Attachment A, if applicable.
2. Receipt of appropriate fees – Refer to Fee Schedule
3. Proof of submission of fingerprints (Copy of BCII 8016, Request for Live Scan Services or FD 258, Fingerprint Hard Card) for individuals designated as having secure access, submission of fingerprinting fees and determination of no disqualifying offenses
4. Submission of a copy of the vendor's Secretary of State Certificate of Status. (Refer to ERDS 0003, to Section B of Application for Vendor of Software Certification), if applicant is an approved CMAS vendor.
5. In order to obtain approval of software, a Vendor of Software must read Section C, ERDS 0003, Application for Vendor of Software Certification, and certify and sign, under penalty of perjury, that the software meets the Baseline Requirements and Technology Standards established by the Attorney General. The approval of the software certificate will include a "disclaimer" stating that the software is not being approved as to its ability to serve/function in an ERDS operational environment nor that it meets all County Recorder's requirements; only that the vendor has stated that it meets the Department of Justice Baseline Requirements and Technology Standards as of the date of the AG's software approval.
6. To qualify to apply for Vendor of Software Certification, the applicant must provide either:

    a. Three (3) best references within the last five (5) years for software products or development of equivalent technology, complexity, and size of

an electronic recording delivery system. At least one (1) reference shall be for a project using document-imaging technology. ERDS 0009, Vendor Application Form for Reference(s), Attachment B, is provided for completion of this information.

OR

b. A Vendor with a valid California Master Services Agreement (CMAS), General Services Agreement (GSA), or Master Services Agreement (MSA) may submit a copy of this agreement in lieu of the above references. The CMAS, GSA, or MSA must include one or more of the following service categories:

- Consulting-Application Development
- Consulting-IT Acquisition Support
- Consulting-IT Project Management
- Consulting-IT Project Planning
- Consulting-IT Strategic Planning
- Consulting-IT System Implementation
- Consulting-Migration Planning
- Consulting-Software Development
- Consulting-System Analysis
- Consulting-System Design
- Consulting-System Development
- Consulting-System Integration

Upon receipt of the application, the ERDS Program will verify that the above criteria has been met and will initiate the processing of the application.

SECTION 6
APPLICATION PROCESSING

The ERDS program will respond to vendor with an approval or denial within an estimated timeframe of 90 days of receipt of the application and all associated documents.

One of the following steps will be taken following Department of Justice's review of the ERDS 0003, Application for Vendor of Software Certification.

A. If the application is determined to be incomplete:

An incomplete application is determined by the following criteria
1. Rejected fingerprints
2. Missing/illegible data
3. Incorrect/missing fees

ERDS Program will:

Return the application to the applicant with a cover letter explaining the reason for return.

Applicant will:

Have thirty (30) days to respond.
If the applicant does not respond within thirty (30) days, the application shall be considered void. Any subsequent application shall require submission of new fees.

Note: Within the thirty (30) days, the estimated Department of Justice response timeframe of ninety (90) days is suspended until the application has been resubmitted and received by the ERDS Program.

B. If the application is determined to successfully meet all criteria:

I. Approval of application for Vendor of Software Certification:

ERDS Program will proceed by:
1. Issuing an Approval Letter
2. Issuing a Certificate of Vendor of Software Certification

The certificate will reflect the following:
- Date of Issuance
- Expiration Date
- Vendor Name

- Vendor Certification Number

NOTE: Issuance of a Vendor Certificate does not supersede any of a County Recorder's contracting requirements.

II. Approval of Software Notification:

ERDS Program will proceed by:
1. Issuing an Approval Letter
2. Issuing a Software Approval Certificate

The certificate will reflect the following:
- Date of Issuance
- Expiration Date
- Vendor Name
- Vendor Certification Number

NOTE: The approval of the software certificate will include a "disclaimer" stating that the software is not being approved as to serve/function in an ERDS operational environment nor that it meets all County Recorder's requirements; only that the vendor has stated that it meets the Department of Justice Baseline Requirements and Technology Standards as of the date of the AG's software approval.

C. If the application is determined to be denied:

ERDS Program will proceed by:
1. Issuing a letter of denial, informing the applicant of the reason for denial.

Refer to Section 9 – APPEAL PROCESS

SECTION 7
VENDOR RENEWAL

The Certificate of a Vendor of Software, as issued by the Department of Justice to the vendor, including those designated employees and/or business entities of the vendor, shall remain in effect for a period of three (3) years unless termination has been issued to the individual by the Department of Justice. An ERDS 0003, Application for Vendor of Software Certification indicating Renewal shall be submitted to the Department of Justice at the end of the three (3) year period for vendors wishing to renew their certification.

SECTION 8
TERMINATE, SUSPEND OR WITHDRAWAL

Termination / Suspend:

A County Recorder may refuse to enter into a contract with any party or may terminate or suspend access to a system for any good faith reason. Government Code section 27391(c). The County Recorder will make notification to Department of Justice in the case of a termination or suspension. Government Code section 27394 (f).

In addition to a County Recorder's notification of termination or suspension, the Department of Justice shall terminate or suspend an approval based on a subsequent notification of a disqualifying offense and/or any breaches of ERDS security Government Code section 27395 (a) and Government Code section 27396(a).

For the purpose of ERDS processes, the terms "terminate" and "suspend" are considered interchangeable and are used to designate removal of all privileges of access.

Department of Justice shall issue a letter of termination or suspension to the vendor notifying that Department of Justice certification is invalid.

Department of Justice shall issue a letter to the County Recorder notifying him/her of such termination or suspension and instructing that the County Recorder remove all means of access for the terminated or suspended individual using any login credentials or digital certificates provided for access.

To appeal a termination or suspension, refer to Section 9 – Appeal Process.

Withdrawal from Vendor Certification

A Vendor of Software choosing to withdraw their Vendor Certification shall submit a completed ERDS 0010, Application for Withdrawal, to the Department of Justice.

Department of Justice shall issue a letter of Vendor Certification Termination to the Vendor; notifying he/she that the Department of Justice certification has been withdrawn.

Department of Justice shall issue a letter to the County Recorder notifying him/her of such withdrawal and instructing that the County Recorder remove all means of Vendor access.

All Vendor of Software Certification fees are non-refundable. If at a later date, the Vendor chooses to have his/her Vendor of Software Certification re-instated, the Vendor must re-apply and complete the application process including payment of fees. The Vendor will be issued a new Certification Number.

The Vendor will retain his/her secure access status unless approval has expired or has been terminated or suspended by the County Recorder or the Department of Justice.

SECTION 9
APPEAL PROCESS

The following steps are available based on either denial of an application or termination/suspension of a certificate.

A. Denial of Application

A denial must be appealed in writing within thirty (30) days of the ERDS Program notification to the applicant:

- A program committee will review a request for an Appeal.
- A determination shall be made in writing to the appellant:

  Appeal denied – ERDS staff shall issue a letter informing the appellant.

  Appeal granted – ERDS staff shall issue a letter informing the appellant of the decision to grant the appeal.

B. Termination or Suspension of Certification

A termination or suspension of a certification must be appealed in writing within thirty (30) days of the ERDS program notification to the certificate holder:

- A program committee shall review a request for an Appeal.
- A determination shall be made in writing to the appellant:

  Appeal denied – ERDS staff shall issue a letter informing the appellant.

  Appeal granted – ERDS staff shall issue a letter informing the appellant of the decision to grant the appeal.

SECTION 10
REQUEST FOR REPLACEMENT CERTIFICATE AND/OR COPIES

ERDS 0006, Request for Replacement of Certificate or Application Documents is to be utilized for requesting the documents listed below.

Duplicate Certificate:

A vendor may request a duplicate Certificate of Vendor of Software Certification or an Approved Software Certificate for the following reasons. The appropriate fee must accompany the request. (Refer to Fee Schedule)

1. A certificate has been lost, stolen or destroyed.
2. A certificate has been mutilated and is no longer usable.
3. Non-receipt of the original certificate.
4. Change in name and/or address reflected on original certificate.

Request for Copies:

A vendor may request copies of documents pertaining to his/her application that are designated as public documents. The request shall be accompanied by the appropriate fee. (Refer to Fee Schedule)

1. Application for Vendor of Software Certification
2. All documents on file

SECTION 11
ESCROW REQUIREMENTS

A Vendor of a County Recorder's ERDS is required to place the ERDS source code and other materials in an approved Escrow Facility. This section establishes the escrow requirements to be met.

Approved Escrow Facility

An Escrow Company approved pursuant to California Code of Regulations, Title 2, beginning with Section 20630.

Escrow Requirements

Electronic recording delivery system software program source code(s) (or hereinafter: "source code") shall be placed in escrow in order to:

(a) Create a record of all versions, including changes or modifications of the source code materials placed in escrow;
(b) Create a record of all applications for access to the source code materials placed in escrow;
(c) Unless otherwise superseded by a contract between a vendor and a county recorder, preserve the necessary source code information to permit the county recorder to continue the use and maintenance of the source code in the event the vendor is unable, or otherwise fails, to provide maintenance.

Electronic Recording Delivery System Program Source Code(s)

"Electronic recording delivery system software program source code(s)" or "source code" consists of the computer program or programs used for the delivery for recording, and return to the party requesting recording, of a digitized electronic record that is an instrument affecting a right, title, or interest in real property or a digital electronic record that is an instrument of reconveyance, substitution of trustee, or assignment of deed of trust and store that digitized or digital electronic record to a storage media for later retrieval and reporting

Vendor Letter of Deposit

Within a timeframe established by the County Recorder of any submission of source code materials by a vendor to an approved escrow facility, the vendor shall acknowledge in writing to the affected County Recorder that they have placed their source code or codes

in escrow. The vendor letter of deposit shall include a description of submitted materials sufficient to distinguish them from all other submissions.

The vendor letter of deposit shall state:

(1) That all source code information and materials required by these regulations and other applicable law are included in the deposit.
(2) The name of the approved escrow company and the location of the escrow facility where the source code materials have been placed in escrow. The escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.
(3) The escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.
(4) That the escrow company meets the "requirements for escrow facility" as stated in the Escrow Requirements.

Requirements for Submission

(a) The vendor shall submit the source code, as defined in (c) below, to an approved escrow company for placement in the escrow facility.
(b) For each source code, the materials placed in escrow must be sufficient to maintain every related electronic software program used or intended to be used by any county recorder.
(c) The content of escrow materials should be compiled to allow complete and successful restoration of the ERDS in its production environment with confirmation by a production verification test by qualified personnel using only this content. It should include, but not limited, to the following items:

(1) All software modules-components purchased by the Vendor, and used in building the ERDS.
(2) All licenses and security license keys necessary for successful installation and use of these components.
(3) Full documentation (functional descriptions, interface specifications, instructions for installations and use) for all purchased components from their original manufacturers.
(4) Technical support and warranty information from original manufacturers of the components.
(5) Architectural documentation showing usage of these components in the built ERDS.
(6) All software modules-components (in original source code version) developed by the Vendor and used in building the ERDS.
(7) Full engineering design documentation (diagrams, dictionaries, specifications, unit test scripts) for each developed component.
(8) System architectural design documentation.
(9) Bill of Materials – detailed list of all system components purchased and developed.

(10) Detailed deployment diagrams for production environment and deployment specifications with all "build" and "make" instructions.
(11) Detailed Deployment Plan specifications.
(12) Installation and deployment scripts, configuration files, data definition language scripts, and other instructions necessary for full install of the ERDS.
(13) Data loads used for initiation of production with loading scripts or harnesses.
(14) Production Verification Test (content and expected results).
(15) Copy of all compilers and other deployment tools, if purchased separately from OS software, used with their versions mentioned.
(16) Copy of Operating System "sysgen" instructions used for platform preparations for ERDS deployment at different nodes.
(17) Copy of all OS patches used for platform preparations for ERDS deployment at different nodes.

Updates to Submission

Once used to record a digital or digitized record in any electronic recording delivery system, no source code materials in escrow may be changed or modified. Substantive Modifications as described below requires that a new escrow be established.

Substantive Modifications

The following defines substantive modifications:

(1) To source code –
- Modifications or changes leading to a different functional behavior of ERDS or its part (application)
- Modifications of call signatures in interfaces with purchased components
- Modifications of data structures or structural database objects (add table or add column to a table)
- Any change that require modification of deployment procedures.

(2) To Compilers –
- New version of a compiler is as a substantive modification, if the existing ERDS source code can not be compiled error free (including warnings) without changes of the source code.

(3) To related software (i.e., libraries or purchased components) –
- Any change in a component or module functionality
- Any change in call signatures of modules or call interfaces

(4) To an operating system –
- Any change or upgrade that relates to security settings or security policies
- Cumulative update to a new service pack level

(5) To a System and/or network devices
- Any changes to the server, workstation and/or network devise hardware/software configuration that impacts the ERDS system.

- Any changes to the network architecture/network design as it pertains to the ERDS.

Elaboration: If an ERDS is designed to be independent of the operating system, only ERDS source code needs to be tested, archived and escrowed. For ERDS application source code, any modification is substantive and must be tested, archived and escrowed. If an ERDS cannot be designed to be independent of the operating system, then for any operating system, compiler or related software (i.e. libraries), any patch or "hotfix" that corrects one or more vulnerabilities, at least one of which presents "high risk" of system compromise, must be considered "substantive". Such a patch or hotfix must be archived and escrowed to ensure subsequent installations using the original operating system are properly patched.

Deposit Software Modifications into Escrow

(a) Prior to being used to record digital or digitized documents in any electronic recording delivery system, the vendor shall submit all source code changes or modifications into escrow in the same manner and under the same conditions in which the source code materials originally were placed in escrow.

(b) Within a timeframe established by the County Recorder of any submission of changed or modified source code, the vendor shall notify each affected County Recorder that the source code placed in escrow has been changed or modified.

Separation of Interest of Escrow Company with Vendor

A vendor may enter into a written agreement with any escrow company for deposit of each source code. However, the escrow company, its officers, and directors, shall not hold or exercise any direct or indirect financial interest(s) in the vendor.

Requirements for Escrow Facilities

For all electronic recording delivery system software program source code materials each escrow facility shall:
(a) Provide a secure and safe environment in which the humidity, temperature, and air filtration are controlled on a 24-hours-a-day, 7-days-a-week basis. The humidity shall be maintained at 35 percent, plus or minus 2 percent, and the temperature shall be maintained at 65 degrees, plus or minus 3 degrees, Fahrenheit.
(b) Maintain storage away from electrical, magnetic, and other fields which could potentially damage computer media over time.
(c) Have backup capability to maintain the properly secured environment in the event of power outages or natural disasters.

(d) Maintain physical security of the escrow facility with controlled and restricted access to all materials placed in escrow.
(e) Store each source code separately. The source code materials placed in escrow shall be secured in a single container and no other material shall be placed in that container.

Conditions for Access to Materials Placed in Escrow

No access to materials placed in escrow shall occur except as specified in this section.
(a) County Recorder shall provide and maintain a list of people having access to escrow materials. Escrow facility will keep a log of access to the materials stored.
(b) Upon a finding by the Attorney General, county recorder, or district attorney that an escrow facility or escrow company is unable or unwilling to maintain materials in escrow in compliance with these regulations.
(c) The Attorney General may, in furtherance of these regulations, for cause at any time, audit source code materials placed in escrow with an escrow facility for purposes of verifying the contents.
(d) An approved computer security auditor shall have access to any aspect of an electronic recording delivery system, in any form requested to complete their certification of the system. Computer security auditor access shall include, but not be limited to, permission for a thorough examination of source code and the associated approved escrow facility, and necessary authorization and assistance for a penetration study of that system.
(e) The vendor shall be entitled at reasonable times during normal business hours and upon reasonable notice to the escrow company during the term of the escrow agreement to inspect the records of the escrow company pertaining to the escrow agreement.

Integrity of Materials Placed in Escrow

No person having access to the electronic recording delivery system software program source code materials shall interfere with or prevent the escrow representative from monitoring the security and the integrity of the electronic delivery system software program source code materials.

Minimum Terms Required in Agreement

The terms of the agreement between the vendor and the escrow company shall include, but not be limited to, the following elements:

(1) The escrow company, its officers, and directors, do not hold or exercise any direct or indirect financial interest(s) in the vendor.

(2) The vendor, its officer, and directors, do not hold or exercise any direct or indirect financial interest(s) in this escrow company.

(3) No source code placed in escrow shall be changed or modified except as permitted in this chapter.

(4) The time period for the escrow agreement and the date for renewal of the agreement.

(5) A provision that the escrow agreement may be renewed for additional periods.

(6) The due date for renewal shall be no later than 30 days before expiration of the escrow agreement. In the event that the contract is not renewed, the escrow company shall so notify the County Recorder and the Attorney General.

(7) In the event that a vendor does not enter into an escrow arrangement with the escrow company to renew the escrow contract, a County Recorder may negotiate directly with an escrow company for continuance of the escrow, and shall so notify the Attorney General and the vendor in writing within 30 days of the new contract.

(8) In the event that the escrow company is notified by a county recorder of the occurrence of a condition as defined in the escrow agreement allowing access to electronic recording delivery system software program source code materials, the escrow company shall immediately so notify the vendor and the Attorney General and shall provide a copy of the notice from the county recorder.

(9) If the vendor provides an objection in writing within 10 days of the mailing or other service of the notice to the vendor, the escrow company shall not allow access. If the vendor does not object as provided in this subdivision, the escrow company shall permit access to the deposit to the county recorder. For the purposes of this section "object" or "objection" means the delivery by certified mail of an affidavit or declaration to the escrow company by the vendor, with a copy to the county recorder which is demanding access and a copy to the Attorney General. The objection shall state that an access condition either has not occurred or no longer exists. Upon receipt of the objection, the escrow company shall not permit access and shall continue to store the deposit pursuant to the escrow agreement.

(10) A requirement that the Escrow company submit a copy of every electronic recording delivery system escrow agreement to the County Recorder. The copy shall be submitted by the escrow company within ten days of the date the escrow agreement is signed.

(11) For every submission of an electronic recording delivery system escrow agreement, maintain records which sufficiently identify and describe the materials deposited in escrow to determine compliance with the agreement between the

vendor and the escrow company. The escrow company shall not be required to verify the content of the materials submitted.

(12) Notify, in writing, the County Recorder within five days of the initial deposit of electronic recording delivery system source code. The notice shall include the name of the vendor and a list describing each of the items comprising the initial submission.

(13) Notify, in writing, the County Recorder within five days of the termination of any electronic recording delivery system escrow agreement.

(14) Notify, in writing, the Attorney General within five days of the change of the name of the company or the name of the escrow facility, together with the address, phone number, and name of the contact person for the company and/or facility.

Retention of Electronic Recording Delivery System Materials

Records maintained by the escrow company pursuant to these regulations and other applicable law shall be retained for the term of the escrow agreement, and for an additional period of 22 months.

The escrow agreement shall provide for the disposition of the materials placed in escrow.

State Not Liable for Any Costs or Any Other's Actions

Neither the Attorney General nor the State of California shall be responsible for any of the fees claimed by the vendor, election jurisdictions, or the escrow company to establish the escrow contract. Further, neither the Attorney General nor the State of California is a party to the agreement and shall not incur any liability for the actions of the parties involved in this escrow agreement.

SECTION 12
SECURITY AUDIT REQUIREMENTS

Nature and Frequency of Electronic Recording Delivery System Computer Security Audits

An initial audit is required before any Electronic Recording Delivery System may be implemented. An approved Computer Security Auditor shall conduct a security audit of a County Recorders Electronic Recording Delivery System and it's Authorized Submitter(s) for the purpose of validating that the system is reasonably secure from vulnerabilities and unauthorized penetration.

Thereafter, an ERDS Approved Computer Security Auditor shall audit the Electronic Recording Delivery System annually for the system to remain certified and whenever a substantive modification is made to the Electronic Recording Delivery System.

A computer security audit is a systematic, measurable, technical assessment of how the baseline security requirements required by the Attorney General are applied to an Electronic Recording Delivery System.

Security Audit for Initial Implementation and Substantive Modification

The approved Computer Security Auditor shall conduct an end-to-end security audit of the Electronic Recording Delivery System in accordance with generally accepted information security practices. The approved Computer Security Auditor must document his/her findings during the audit. Information in an audit report shall include, but is not necessarily limited to, the following:

1. Demonstration of the proposed system in its intended operational environment in a test mode. Testing shall include the following:

    - A review of the network configuration showing all network nodes;
    - An inventory of hardware, software and network components comprising the proposed system;
    - An inventory of users and roles assigned to operate the system;
    - Tests showing that digital and digitized documents are neither transmitted nor stored in an unencrypted format anywhere in the system.
    - Tests showing that transmissions only occur between authorized parties. The operational environment must be mapped to identify (a) the servers, workstations and network nodes visible from any ERDS workstation or server, (b) the ERDS workstations and servers visible from any non-ERDS workstation or server, and (c) the users and roles authorized to access ERDS workstations and servers.
    - Remnants of sessions, transmissions and documents are not stored once the user initiating the session and transmitting documents has logged out or been disconnected (either physically or logically).

- A review of the system design showing all components;
- A review of the source code or selected (or all) software components;
- The test environment must simulate authorized and unauthorized users operating in the roles of county recorder, authorized submitter, agent of authorized submitter, and Internet user.

2. A Description of Deposit Materials showing that the source code has been deposited in Escrow with an Escrow Company approved pursuant to Chapter 6, Division 7, Title 2 of the California Administrative Code, beginning with Section 20630.

Annual Audit

The County Recorder shall obtain an audit of the Electronic Recording Delivery System at least once every year. An authorized Computer Security Auditor must perform the audit. The audit will be conducted in the system's operational environment. Testing shall include the following:

1. A review of the network configuration showing all network nodes;
2. An inventory of hardware, software and network components comprising the proposed system;
3. An inventory of users and roles assigned to operate the system;
4. Tests showing that digital and digitized documents are neither transmitted nor stored in an unencrypted format anywhere in the system.
5. Tests showing that transmissions only occur between authorized parties. The operational environment must be mapped to identify (a) the servers, workstations and network nodes visible from any ERDS workstation or server, (b) the ERDS workstations and servers visible from any non-ERDS workstation or server, and (c) the users and roles authorized to access ERDS workstations and servers.
6. Remnants of sessions, transmissions and documents are not stored once the user initiating the session and transmitting documents has logged out or been disconnected (either physically or logically).
7. Collected audit data correlates to actual activity and all auditable events are collected for audit.
8. Description of Deposit Materials showing that the source code has been deposited in Escrow with an approved Escrow Company.

Audit Report Format

The format for both the Initial and Annual Security Audit shall include, but is not necessarily limited to, the following:

1. A non-technical, business-oriented executive overview.

2. A detailed technical observation/recommendation section.

3. A summary of recommendations in a task-list format.

4. A ranking of the vulnerabilities/weaknesses found during the audit will be documented utilizing a High, Medium, and Low level-of-risk categorization. Show a correlation of each security vulnerability/weakness to a business risk.

    - High-level vulnerabilities/weaknesses will be classified as vulnerabilities/weaknesses found to pose a hazardous level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.
    - Medium-level vulnerabilities/weaknesses will be classified as vulnerabilities/weaknesses that pose a significant level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.
    - Low-level vulnerabilities/weaknesses will be classified as vulnerabilities/weaknesses that do not pose a significant level of risk to the confidentiality, integrity and/or availability of the data and services provided by the ERDS.

5. A diagram depicting results where applicable.

6. A description of the approved Computer Security Auditors methodology.

7. A recommendation for any additional precautions needed to ensure that the system is secure.

The initial security audit report shall be further subdivided and include but will not be limited to the following categories of items:

Audit Categories	System Passes/Fails	Comments, Notes
Safety and security of the system:		
No evidence of breaches during testing		
System performed to specifications		
Physical security measures are adequate to prevent unauthorized access		
User survey conducted with satisfactory results in security confidence		
Vulnerability of the electronic recording delivery system to fraud or penetration:		
All documents entering and exiting the system were encrypted per ERDS requirements		
Mechanisms for encrypting met the ERDS Baseline Requirements and Technology Standards		
Access control measures acted to restrict		

access based on identity and organizational role		
Authentication correctly identified authorized users		
Satisfactory testing conducted submitting sample documents from location X		
Results of testing of the system's protections against fraud or intrusion, including security testing and penetration studies:		
Penetration testing concluded that the system was not exploitable based on the tests conducted		
Security events were properly recorded and detected in audit logs		
Recommendations for any additional precautions needed to ensure that the system is secure:		
Auditor recommends timing of audits increase/decrease		
Encryption keys should be increased by X		
The organization needs to add to or improve security policies		
Recommendation to add more constrictive controls		
Recommendation to authorize continued use		

System Authorization Decision

Audit findings shall be conveyed to the County Recorder in a written audit report. The initial audit report shall be attached to the ERDS 0001, Application for System Certification, submitted by the County Recorder when applying with Department of Justice for system certification. Thereafter, an annual audit report will be forwarded by the County Recorder to the Department of Justice consistent with the Terms and Conditions-System Certification. There are two types of decisions that can be rendered by the Department of Justice:

1. Authorization to operate; and

2. Denial of authorization to operate.

Authorization to Operate

If, after assessing the results of the Computer Security Audit, the Department of Justice deems that the Electronic Recording Delivery System has met the Baseline Requirements and Technology Standards established for an Electronic Recording Delivery System with no high-level or medium-level vulnerabilities/weaknesses, an authorization to operate

will be issued for the Electronic Recording Delivery System. The authorization will indicate that the Electronic Recording Delivery System is authorized to operate without any significant restrictions or limitations on its operation.

Although not affecting the authorization to operate decision, the County Recorder should take specific actions to reduce or eliminate any low-level vulnerabilities/weaknesses identified by the Computer Security Auditor where it is cost-effective to do so. The County Recorder shall, as the system owner, establish a disciplined and structured process to monitor the effectiveness of the security controls for the Electronic Recording Delivery System.

Denial of Authorization to Operate

If, after assessing the results of the Computer Security Audit, the Attorney Generals authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable, the authorization to operate the Electronic Recording Delivery System will be denied. The system will not be certified and will not be placed into operation. If the system is currently in operation, all activity shall be halted.

To address the security related deficiencies the County Recorder shall submit a plan of action and milestones to be used by the Department of Justice and Computer Security Auditor to monitor the progress in correcting deficiencies noted during the security audit.

When the security related deficiencies have been addressed and confirmed by the Computer Security Auditor, the County Recorder may request the Department of Justice for reconsideration for authorization to operate and system certification.

The County Recorder shall, as the system owner, establish a disciplined and structured process to monitor the effectiveness of the security controls for the Electronic Recording Delivery System.

Filing Procedures

Upon completion, the final Computer Security Auditors "Security Audit Report", the Attorney Generals "System Certification Decision" recommendation and any response to any recommendations shall be transmitted to the board of supervisors, the county recorder, the county district attorney, and the Attorney General. These reports shall be exempt from disclosure under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title1).

SECTION 13
APPENDICES/FORMS

The Appendices include the following documents:

Terms and Conditions – Vendor
Social Security Number Privacy Statement
Fee Schedule - PENDING
Disqualifying Offenses
Statutory Authority, Chapter 621
Statutory Authority, Chapter 520
Regulations – PENDING
Baseline Requirements and Technology Standards

TERMS AND CONDITIONS - VENDOR

Electronic Recording Delivery System Vendor of Software must review, understand and agree to the Terms and Conditions Statement to obtain Vendor Certification by the Department of Justice Electronic Recording Delivery System Program. The Terms and Conditions include the requirement to protect the confidentiality, integrity, and availability of the electronic recording delivery system.

1. Scope
    - The Terms and Conditions - Vendor apply to all personnel, equipment, software, systems, networks, communication links, and facilities supporting and/or acting on behalf of the certified Vendor of Software.
    - These Terms and Conditions do not confer, grant, or authorize any rights or privileges to any entity or person other than the certified Vendor of Software and/or those acting on the behalf of the certified Vendor of Software.

2. Personnel Security

    - The Certified Vendor of Software shall be responsible for the actions of any person or entity acting on their behalf and/or providing services in support of the certified Vendor of Software.
    - All employees and/or business entities acting on behalf of the vendor shall be subject to the fingerprint background requirements prior to a vendor's certification.
        - The Certified Vendor of Software shall maintain a current list of all personnel and/or business entities employed by and/or acting on their behalf that have been granted secure and/or authorized access to any electronic recording delivery system.

3. Site Security

    - The site housing all hardware and software associated with the capture, development and/or transmission of electronic recording delivery system security testing and audit reports shall be adequately secured at all times to reasonably protect against theft, damage, and/or unauthorized access or use by any person.

4. Information Security

    - The data residing in the electronic recording delivery system is confidential and the use of this information for any purpose other than the purpose for which it was expressly provided is strictly prohibited. Violation of the electronic recording delivery system security may subject the certified Vendor of Software and/or those acting on the behalf of the

certified Vendor of Software to criminal and/or civil liability, and may result in termination of the Vendor of Software certification.
Every person as designated by a County Recorder who, in the course of their normal duties collects, processes, and/or facilitates the capture, development and/or transmission of electronic recording delivery system data shall be required to sign an ERDS 0011, Secure and Authorized Access Statment, as provided by the County Recorder acknowledging that they understand their responsibilities for protecting confidential electronic recording delivery system information, the restrictions concerning the use of such information, and the penalties for misuse. Signed copies of the Certification form shall be retained by the County Recorder and shall be made available to the Attorney General upon request.

- Vendor agrees to maintain policies and procedures in accordance with NIST SP 800-53. To review NIST SP 800-53 go to: **http://csrc.nist.gov/publications/nistpubs/index.html**

5. Security Violations

- All security violations or suspected security violations shall be immediately reported to the Attorney General. Reports of security violations shall include the date of the incident(s), the parties involved (if known), the nature and scope of the incident, and any action(s) taken, including steps to protect against future violations.
·The Attorney General reserves the right to investigate all reported or suspected security violations and to take any action deemed appropriate and/or necessary to protect the security and stability of the electronic delivery system, including termination of the Vendor of Software certification.

6. Quality Control

- All equipment associated with the capture and transmission of electronic recording delivery systems information shall be adequately secured at all times by assuring that software upgrades (including the installation of any patches deemed necessary by the manufacturer) shall be applied in a timely fashion and shall remain current.

SOCIAL SECURITY NUMBER
PRIVACY STATEMENT

USE OF SOCIAL SECURITY NUMBER: You are required by law to provide your Social Security Number (SSN) or your application will not be processed for the ERDS Certification.

The SSN is required and will be used by the Department of Justice (DOJ) for identification and verification purpose. The SSN provided on the application will not be made available for the public inspection. The SSN is a standard data element included in the DOJ criminal offender record information systems as defined in Penal Code section 13125. In addition, Family Code section 17520 requires that any state Department issuing certificates to engage in an occupation shall collect the SSN of the applicant.

Collection of you SSN is mandatory. Failure to provide the information will result in the rejection of your application for certification.

I have read the Privacy Statement and understand the Privacy Statement information.

Signature: _____ Date _____

Print name: _____

Applicant should keep a copy of this for their record.

FEE SCHEDULE

Process	Fee	Trans Code ASD to assign	Trans Title (for DOJ use only)	Fund
Vendor				
Initial Vendor and Software Certification	TBD			Electronic Recording Authorization Account
Renewal Certification	TBD			Electronic Recording Authorization Account
County				
System Administration Fee	This fee is allocated to each participating county by the total documents recorded and filed as reported to the Office of the Insurance Commissioner, as provided in Government Code section 27296, for the previous year. The formula to determine a county's proportionate cost is set by the total documents recorded and filed per individual participating counties divided by the total documents recorded and filed by all participating counties. The percentage figure obtained for each participating county is applied to the estimated annual costs of the Attorney General to arrive at an individual participating county figure.			Electronic Recording Authorization Account
MISC				
Fingerprint (State) Hard Card & Live Scan	$32.00			Fingerprinting Fee Account
Fingerprint (Fed) Hard Card & Live Scan	$24.00			Fingerprinting Fee Account
Returned Item (DOJ Manual 13230)	$10.00			Electronic Recording Authorization Account
Re-issuance of Certification (lost/destroyed)	$10.00			Electronic Recording Authorization Account
Copies (Admin Bulletin 05-08)	.30 per page			Electronic Recording Authorization Account

ELECTRONIC RECORDING DELIVERY SYSTEM
SECURE ACCESS
DISQUALIFYING OFFENSES

For the purposes of fingerprinting, Secure Access[1] refers to an individual's ability to submit documents for recording in a digitized environment. No person shall be granted secure access to an electronic recording delivery system if he or she has been convicted of a felony, has been convicted of a misdemeanor related to theft, fraud, or a crime of moral turpitude, or if he or she has pending criminal charges for any of these crimes. A plea of guilty or no contest, a verdict resulting in conviction, or the forfeiture of bail, shall be a conviction within the meaning of GC section, 27395 (a), irrespective of a subsequent order under Section 1203.4 of the Penal Code.

A felony conviction or pending charges involving the following offenses will be justification for denial of secure access:

Felony:

• Homicide	• Forgery
• Robbery	• Arson
• Assault	• Drugs
• Kidnapping	• Sex
• Burglary	• Driving under the Influence
• Theft	• Hit and Run
• Motor Vehicle Theft	• Weapons
• Escape	• Bookmaking
• Identity Theft	• Unauthorized Access to Computers

And/Or

Any other state or federal felony convictions including pending charges, involving dishonesty, fraud or deceit, which are substantially related to the qualifications, functions, or duties of a person engaged in the secure access of an electronic recording delivery system as described within Government Code Sections 27390-27399.

A misdemeanor conviction or pending charges involving the following offenses will be justification for denial of secure access:

Misdemeanor:

• Misdemeanor manslaughter	• Liquor Laws
• Assault and Battery	• Disturbing the Peace
• Theft	• Malicious Mischief
• Drugs	• Driving under the Influence
• Sex	• Gambling
• Checks and Access Cards	• Trespassing
• Vandalism	• Contributing to the delinquency of a minor
• Identity Theft	• Unauthorized Access to Computers

And/Or

Any other state or federal felony convictions, including pending charges, involving "moral turpitude" [People v. Castro (1985) 38 Cal. 3d 301], provided that the crimes are substantially related to qualifications, functions, or duties of a person engaged in the secure access of an electronic recording delivery system as described within Government Code Sections 27390-27399. Examples of crimes involving moral turpitude include murder, rape, assault with a deadly weapon, hit-and-run, arson, robbery, burglary, possession of drugs for sale, sale of drugs, pimping and pandering, etc.

---

[1] The fingerprint requirement does not apply to an individual who has been granted 'authorized access' and who is limited to submitting digital documents only; however, all individuals granted 'Secure Access' or 'Authorized Access' by a County Recorder must sign ERDS 0005, Application Attachment Vendor Employee(s) and/or Business Entity(ies) Attachment A.

Assembly Bill No. 578

CHAPTER 621

An act to add Article 6 (commencing with Section 27390) to Chapter 6 of Division 2 of Title 3 of the Government Code, relating to county recorders, making an appropriation therefor, and declaring the urgency thereof, to take effect immediately.

[Approved by Governor September 21, 2004. Filed with Secretary of State September 21, 2004.]

LEGISLATIVE COUNSEL'S DIGEST

AB 578, Leno. County recorders: electronic recording.

(1) Existing law generally specifies that the recorder of any county may, in lieu of a written paper, accept for recording a digitized image of a recordable instrument, subject to specified conditions.

This bill would enact the Electronic Recording Delivery Act of 2004, to authorize a county recorder, upon approval by resolution of the board of supervisors and system certification by the Attorney General, to establish an electronic recording delivery system for the delivery for recording of specified digitized and digital electronic records, subject to specified conditions, including system certification, regulation, and oversight by the Attorney General. It would authorize a county recorder to include in its electronic recording delivery system a secure method for accepting for recording a digital or digitized electronic record that is an instrument of reconveyance, substitution of trustee, or assignment of deed of trust, subject to specified conditions. It would require participating counties to pay for the direct cost of regulation and oversight by the Attorney General, and authorize those counties to impose fees to cover those costs. It would authorize the Attorney General to charge a fee directly to a vendor seeking approval of software and other services as part of an electronic recording delivery system. Fees paid to the Attorney General under these provisions would be deposited in the Electronic Recording Authorization Account, which would be created in the Special Deposit Fund and continuously appropriated to the Attorney General for these purposes.

This bill would authorize the Attorney General or a district attorney or city prosecutor to seek specified civil remedies.

The Attorney General would be required to evaluate the electronic recording delivery systems, and report to both houses of the Legislature on or before June 30, 2009.

(2) This bill would declare that it is to take effect immediately as an urgency statute.

Appropriation: yes.

The people of the State of California do enact as follows:

SECTION 1. (a) It is the intent of the Legislature to enact legislation to develop a system to permit the electronic delivery, recording, and return of instruments affecting right, title, or interest in real property.

(b) (1) Except as set forth in subdivision (c), it is the intent of the Legislature that electronic recording be limited in its initial development to the digitized electronic delivery, recording, and return of instruments submitted by a title insurer, underwritten title company, institutional lender, as defined in paragraph (1), (2), or (4) of subdivision (j) of Section 50003 of the Financial Code, or an entity of local, state, or federal government. This will enable county recorders, county district attorneys, and the Attorney General to develop an electronic recording delivery system that will protect property owners and lenders from fraud and identity theft. It is the intent of the Legislature to consider expanding this system to cover additional submitting entities and digital electronic records based on experience with the system.

(2) It is not the intent of the Legislature in limiting electronic recordation of certain documents to digitized electronic delivery, to suggest, and no inference should be drawn, that digital documents pose a greater risk of fraud or identity theft than digitized documents.

(c) It is further the intent of the Legislature to enact legislation to permit, upon certification, a title insurer, underwritten title company, entity of local, state, or federal government, or institutional lender, as defined in subdivision (j) of Section 50003 of the Financial Code, to submit a digitized or digital electronic record that is an instrument of reconveyance, substitution of trustee, or assignment of deed of trust, without meeting specified requirements of this act because these instruments are less likely to result in consumer fraud.

SEC. 2. Article 6 (commencing with Section 27390) is added to Chapter 6 of Division 2 of Title 3 of the Government Code, to read:

Article 6. Electronic Recording Delivery Act of 2004

27390. (a) This article shall be known and may be cited as the Electronic Recording Delivery Act of 2004.

(b) For the purposes of this article, the following definitions shall apply:

(1) ‘‘Authorized submitter’’ means a party that has entered into a contract with a county recorder pursuant to subdivision (b) of Section 27391 and is not disqualified pursuant to Section 27395.

(2) ‘‘Computer security auditor’’ means computer security personnel hired to perform an independent audit of the electronic recording delivery system. The computer security auditor shall be independent of the county recorder and the authorized submitter and shall not be the same contractor hired to establish or participate in a county’s electronic recording delivery system or in the authorized submitter’s portion of that system.

(3) ‘‘Digital electronic record’’ means a record containing information that is created, generated, sent, communicated, received, or stored by electronic means, but not created in original paper form.

(4) ‘‘Digitized electronic record’’ means a scanned image of the original paper document.

(5) ‘‘Electronic recording delivery system’’ means a system to deliver for recording, and to return to the party requesting recording, digitized or digital electronic records.

(6) ‘‘Security testing’’ means an independent security audit by a computer security auditor, including, but not limited to, attempts to penetrate an electronic recording delivery system for the purpose of testing the security of that system.

(7) ‘‘Source code’’ means a program or set of programs, readable and maintainable by humans, translated or interpreted into a form that the electronic recording delivery system can execute.

(8) ‘‘System certification’’ means the issuance of a confirmation letter regarding a county’s electronic recording delivery system by the Attorney General.

27391. (a) Upon approval by resolution of the board of supervisors and system certification by the Attorney General, a county recorder may establish an electronic recording delivery system.

(b) Upon system certification, a county recorder may enter into a contract with a title insurer, as defined in Section 12340.4 of the Insurance Code, underwritten title company, as defined in Section 12340.5 of the Insurance Code, institutional lender, as defined in paragraph (1), (2), or (4) of subdivision (j) of Section 50003 of the Financial Code, or an entity of local, state, or federal government for the delivery for recording, and return to the party requesting recording, of a digitized electronic record that is an instrument affecting a right, title, or interest in real property. The contract may provide for the delivery of documents by an agent. However, the agent shall not be a vendor of electronic recording delivery systems.

(c) A county recorder may refuse to enter into a contract with any party or may terminate or suspend access to a system for any good faith reason, including, but not limited to, a determination by the county recorder that termination or suspension is necessary to protect the public interest, to protect the integrity of public records, or to protect homeowners from financial harm, or if the volume or quality of instruments submitted by the requester is not sufficient to warrant electronic recordation. A county recorder may also terminate or suspend access to a system if a party commits a substantive breach of the contract, the requirements of this article, or the regulations adopted pursuant to this article.

(d) Notwithstanding Section 27321, a county recorder may require a party electronically submitting records to mail a copy of the recorded electronic document to the address specified in the instructions for mailing upon completion of recording.

(e) When a signature is required to be accompanied by a notary's seal or stamp, that requirement is satisfied if the electronic signature of the notary contains all of the following:

(1) The name of the notary.

(2) The words ''Notary Public.''

(3) The name of the county where the bond and oath of office of the notary are filed.

(4) The sequential identification number assigned to the notary, if any.

(5) The sequential identification number assigned to the manufacturer or vendor of the notary's physical or electronic seal, if any.

27392. (a) No electronic recording delivery system may become operational without system certification by the Attorney General. The certification shall affirm that the proposed county system conforms to this article and any regulations adopted pursuant to this article, that security testing has confirmed that the system is secure and that the proposed operating procedures are sufficient to assure the continuing security and lawful operation of that system. The certification may include any agreements between the county recorder and the Attorney General as to the operation of the system, including, but not limited to, the nature and frequency of computer security audits. Certification may be withdrawn for good cause.

(b) The Attorney General shall approve software and other services for electronic recording delivery systems pursuant to regulations adopted as described in paragraph (7) of subdivision (b) of Section 27393.

27393. (a) The Attorney General shall, in consultation with interested parties, adopt regulations for the review, approval, and

oversight of electronic recording delivery systems. Regulations shall be adopted pursuant to the Administrative Procedure Act (Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3). The regulations shall comply with Section 12168.7.

(b) The regulations adopted pursuant to subdivision (a) may include, but need not be limited to, all of the following:

(1) Establishment of baseline technological and procedural specifications for electronic recording delivery systems.

(2) Requirements for security, capacity, reliability, and uniformity.

(3) Requirements as to the nature and frequency of computer security audits.

(4) A statement of a detailed and uniform definition of the term ''source code'' consistent with paragraph (7) of subdivision (b) of Section 27390, and as used in this article, and applicable to each county's electronic recording delivery system.

(5) Requirements for placement of a copy of the operating system, source code, compilers, and all related software associated with each county's electronic recording delivery system in an approved escrow facility prior to that system's first use.

(6) Requirements to ensure that substantive modifications to an operating system, compilers, related software, or source code are approved by the Attorney General.

(7) Procedures for initial certification of vendors offering software and other services to counties for electronic recording delivery systems.

(8) Requirements for system certification and for oversight of approved systems.

(9) Requirements for fingerprinting and criminal records checks required by Section 27395, including a list of employment positions or classifications subject to criminal records checks under subdivision (f) of that section.

(10) Requirements for uniform index information that shall be included in every digitized or digital electronic record.

(11) Requirements for protecting proprietary information accessed pursuant to subdivision (e) of Section 27394 from public disclosure.

(12) Requirements for certification under Section 27397.5.

(c) The Attorney General may promulgate any other regulations necessary to fulfill his or her obligations under this article.

(c) An electronic recording delivery system shall be subject to local inspection and review by the Attorney General. The Attorney General shall furnish a statement of any relevant findings associated with a local inspection of an electronic recording delivery system, to the county recorder and the district attorney of the affected county, and to all technology vendors associated with that system.

27394. (a) To be eligible to establish an electronic recording delivery system, a county recorder shall contract with, and obtain a report from, a computer security auditor selected from a list of computer security auditors approved by the Attorney General.

(b) The Attorney General shall approve computer security auditors on the basis of significant experience in the evaluation and analysis of Internet security design, the conduct of security testing procedures, and specific experience performing Internet penetration studies. The Attorney General shall complete the approval of security auditors within 90 days of a request from a county recorder. The list shall be a public record.

(c) An electronic recording delivery system shall be audited, at least once during the first year of operation and periodically thereafter, as set forth in regulation and in the system certification, by a computer security auditor. The computer security auditor shall conduct security testing of the electronic recording delivery system. The reports of the computer security auditor shall include, but not be limited to, all of the following considerations:

(1) Safety and security of the system, including the vulnerability of the electronic recording delivery system to fraud or penetration.

(2) Results of testing of the system's protections against fraud or intrusion, including security testing and penetration studies.

(3) Recommendations for any additional precautions needed to ensure that the system is secure.

(d) Upon completion, the reports and any response to any recommendations shall be transmitted to the board of supervisors, the county recorder, the county district attorney, and the Attorney General. These reports shall be exempt from disclosure under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1).

(e) A computer security auditor shall have access to any aspect of an electronic recording delivery system, in any form requested. Computer security auditor access shall include, but not be limited to, permission for a thorough examination of source code and the associated approved escrow facility, and necessary authorization and assistance for a penetration study of that system.

(f) If the county recorder, a computer security auditor, a district attorney for a county participating in the electronic recording delivery system, or the Attorney General reasonably believes that an electronic recording delivery system is vulnerable to fraud or intrusion, the county recorder, the board of supervisors, the district attorney, and the Attorney General shall be immediately notified. The county recorder shall immediately take the necessary steps to guard against any compromise

of the electronic recording delivery system, including, if necessary, the suspension of an authorized submitter or of the electronic recording delivery system.

27395. (a) No person shall be a computer security auditor or be granted secure access to an electronic recording delivery system if he or she has been convicted of a felony, has been convicted of a misdemeanor related to theft, fraud, or a crime of moral turpitude, or if he or she has pending criminal charges for any of these crimes. A plea of guilty or no contest, a verdict resulting in conviction, or the forfeiture of bail, shall be a conviction within the meaning of this section, irrespective of a subsequent order under Section 1203.4 of the Penal Code.

(b) All persons entrusted with secure access to an electronic recording delivery system shall submit fingerprints to the Attorney General for a criminal records check according to regulations adopted pursuant to Section 27393.

(c) (1) The Attorney General shall submit to the Department of Justice the fingerprint images and related information of persons with secure access to the electronic recording delivery system and computer security auditors for the purpose of obtaining information as to the existence and nature of a record of state level convictions and arrests for which the Department of Justice establishes that the applicant was released on bail or on his or her own recognizance pending trial.

(2) The Department of Justice shall respond to the Attorney General for criminal offender record information requests submitted pursuant to this section, with information as delineated in subdivision (*l*) of Section 11105 of the Penal Code.

(3) The Attorney General shall request subsequent arrest notification service, pursuant to Section 11105.2 of the Penal Code, for all persons with secure access to the electronic recording delivery system and all computer security auditors.

(d) The Attorney General shall deliver written notification of an individual's ineligibility for access to an electronic recording delivery system to the individual, his or her known employer, the computer security auditor, and the county recorder.

(e) The Department of Justice shall charge a fee sufficient to cover the cost of processing the criminal offender record information request and any other costs incurred pursuant to this section.

(f) The Attorney General shall define ''secure access'' by regulation and by agreement with the county recorder in the system certification.

27396. (a) The Attorney General shall monitor the security of electronic recording delivery systems statewide, in close cooperation with county recorders and public prosecutors. In the event of an emergency involving multiple fraudulent transactions linked to one

county's use of an electronic recording delivery system, the Attorney General may order the suspension of electronic recording delivery systems in any county or in multiple counties, if necessary to protect the security of the system, for a period of up to seven court days. The Attorney General may seek an order from the superior court if it is necessary to extend this order.

(b) (1) The Attorney General, a district attorney, or a city prosecutor may bring an action in the name of the people of the state seeking declaratory or injunctive relief, restitution for damages or economic loss, rescission, or other equitable relief pertaining to any alleged violation of this article or regulations adopted pursuant to this article. Injunctive relief may include, but is not limited to, an order suspending a party from participation in the electronic recording delivery system, on a temporary or permanent basis.

(2) Nothing in this subdivision shall be construed to prevent the Attorney General, a district attorney, or a city prosecutor from seeking legal or equitable relief under any other provision of law.

27397. (a) A county establishing an electronic recording delivery system under this article shall pay for the direct cost of regulation and oversight by the Attorney General.

(b) The Attorney General may charge a fee directly to a vendor seeking approval of software and other services as part of an electronic recording delivery system. The fee shall not exceed the reasonable costs of approving software or other services for vendors.

(c) In order to pay costs under this section, a county may do any of the following:

(1) Impose a fee in an amount up to and including one dollar ($1) for each instrument that is recorded by the county. This fee may, at the county's discretion, be limited to instruments that are recorded pursuant to the electronic recording delivery system.

(2) Impose a fee upon any vendor seeking approval of software and other services as part of an electronic recording delivery system.

(3) Impose a fee upon any person seeking to contract as an authorized submitter.

(d) The total fees assessed by a county recorder pursuant to this section may not exceed the reasonable total costs of the electronic recording delivery system, the review and approval of vendors and potential authorized submitters, security testing as required by this article and the regulations of the Attorney General, and reimbursement to the Attorney General for regulation and oversight of the electronic recording delivery system.

(e) Fees paid to the Attorney General pursuant to subdivisions (a) and (b) shall be deposited in the Electronic Recording Authorization

Account, which is hereby created in the Special Deposit Fund, and, notwithstanding Section 13340, is continuously appropriated, without regard to fiscal years, to the Attorney General for the costs described in those subdivisions.

27397.5. (a) A county recorder may include in the county's electronic recording delivery system a secure method for accepting for recording a digital or digitized electronic record that is an instrument of reconveyance, substitution of trustee, or assignment of deed of trust.

(b) A county recorder may contract with a title insurer, as defined in Section 12340.4 of the Insurance Code, underwritten title company, as defined in Section 12340.5 of the Insurance Code, an entity of state, local, or federal government, or an institutional lender, as defined in Section 50003 of the Financial Code, or their authorized agents, to be an authorized submitter of the documents specified in subdivision (a).

(c) With respect to the electronic submission of the records described in subdivision (a), the requirements that an authorized submitter be subject to a security audit under Section 27394 and a criminal records check under Section 27395 shall not apply where the certification requirements of subdivision (d) have been met.

(d) (1) In order for subdivision (c) to apply, the county recorder and the Attorney General shall certify that the method of submission allowed under the system will not permit an authorized submitter or its employees and agents, or any third party, to modify, manipulate, insert, or delete information in the public record, maintained by the county recorder, or information in electronic records submitted pursuant to subdivision (b) of Section 27391.

(2) Certification under this section may be withdrawn by either the county recorder or the Attorney General at any time either determines that the requirements of this subdivision are not met.

(e) For purposes of this section, an agent of an authorized submitter shall not include a vendor of electronic recording delivery systems.

27398. (a) The Attorney General shall conduct an evaluation of electronic recording delivery systems authorized by this article, and report to both houses of the Legislature on or before June 30, 2009.

(b) It is the intent of the Legislature that the evaluation include an analysis of costs, cost savings, security and real estate fraud prevention, and recommendations as to improvements and possible expansion of the provisions of this article.

(c) The evaluation shall also include a study of the feasibility of expanding the provisions of this article to cover the delivery, recording, and return of other electronic records.

27399. (a) Nothing in this article shall be construed to authorize any state agency to administer any of the processes or procedures

relating to the business of the county recorders of the state in any manner not otherwise specifically set forth in this article.

(b) The authority granted in this article is in addition to any other authority or obligation under state or federal law.

(c) Nothing in this article shall be construed to repeal or affect Section 27279, 27279.1, 27279.2, 27297.6, 27387.1, or 27399.7, or the authority of the Counties of Orange and San Bernardino to act under those provisions.

SEC. 3. This act is an urgency statute necessary for the immediate preservation of the public peace, health, or safety within the meaning of Article IV of the Constitution and shall go into immediate effect. The facts constituting the necessity are:

In order that county recorders may alleviate fiscal constraints by implementing electronic recording delivery systems at the earliest possible time, it is necessary for this act to take effect immediately.

O

Assembly Bill No. 1738

CHAPTER 520

An act to amend Section 27395 of the Government Code, relating to local government.

[Approved by Governor October 4, 2005. Filed with Secretary of State October 4, 2005.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1738, Committee on Local Government. Electronic recordings: computer security auditors.

The Electronic Recording Delivery Act of 2004 authorizes, among other things, a county recorder, upon approval by a resolution of the board of supervisors and system certification by the Attorney General, to establish an electronic recording delivery system for the delivery and recording of specified digitized and digital electronic records, subject to specified conditions, including system certification, regulation, and oversight by the Attorney General.

The act also requires that a computer security auditor who is hired to perform an independent audit of the electronic recording delivery system shall have access to any aspect of the system. The act also requires that no person may be a computer security auditor or be granted secure access to an electronic recording delivery system if he or she has been convicted of a felony, has been convicted of a misdemeanor related to theft, fraud, or a crime of moral turpitude, or if he or she has pending criminal charges for any of these crimes and requires all persons entrusted with secure access to the system to submit their fingerprints to the Attorney General for a criminal records check pursuant to specified procedures to determine whether they are eligible to have access to an electronic recording delivery system.

This bill would specify that for these purposes a person's criminal history information also includes federal convictions and arrests and would require the Department of Justice to forward requests from the Attorney General to the Federal Bureau of Investigation for this information. The bill would also require the Attorney General to review and compile this information to determine the person's eligibility to have access to an electronic recording delivery system and would authorize the Department of Justice to charge a fee to cover the cost of processing federal criminal offender record information.

The people of the State of California do enact as follows:

SECTION 1. Section 27395 of the Government Code is amended to read:

27395. (a) No person shall be a computer security auditor or be granted secure access to an electronic recording delivery system if he or she has been convicted of a felony, has been convicted of a misdemeanor related to theft, fraud, or a crime of moral turpitude, or if he or she has pending criminal charges for any of these crimes. A plea of guilty or no contest, a verdict resulting in conviction, or the forfeiture of bail, shall be a conviction within the meaning of this section, irrespective of a subsequent order under Section 1203.4 of the Penal Code.

(b) All persons entrusted with secure access to an electronic recording delivery system shall submit fingerprints to the Attorney General for a criminal records check according to regulations adopted pursuant to Section 27393.

(c) (1) The Attorney General shall submit to the Department of Justice the fingerprint images and related information of persons with secure access to the electronic recording delivery system and computer security auditors for the purpose of obtaining information as to the existence and nature of a record of state or federal convictions and arrests for which the Department of Justice establishes that the applicant was released on bail or on his or her own recognizance pending trial.

(2) The Department of Justice shall respond to the Attorney General for criminal offender record information requests submitted pursuant to this section, with information as delineated in subdivision (*l*) of Section 11105 of the Penal Code.

(3) The Department of Justice shall forward requests from the Attorney General to the Federal Bureau of Investigation for federal summary criminal history information pursuant to this section.

(4) The Attorney General shall review and compile the information from the Department of Justice and the Federal Bureau of Investigation to determine whether a person is eligible to access an electronic recording delivery system pursuant to this article.

(5) The Attorney General shall request subsequent arrest notification service, pursuant to Section 11105.2 of the Penal Code, for all persons with secure access to the electronic recording delivery system and all computer security auditors.

(d) The Attorney General shall deliver written notification of an individual's ineligibility for access to an electronic recording delivery system to the individual, his or her known employer, the computer security auditor, and the county recorder.

(e) The Department of Justice shall charge a fee sufficient to cover the cost of processing a state or federal criminal offender record information request and any other costs incurred pursuant to this section.

(f) The Attorney General shall define "secure access" by regulation and by agreement with the county recorder in the system certification.

O

INSERT REGULATIONS HERE

INSERT BASELINE REQUIRMENTS AND TECHNOLOGY STANDARDS HERE

Forms ERDS Requirements Document

This identifies who has responsibility for the completion of and/or submission of the following forms:

Form Name	Vendor	Computer Security Auditor	County Recorder
ERDS 0001 - Application for System Certification			X
ERDS 0002 - Application for Computer Security Auditor Approval		X	
ERDS 0003 - Application for Vendor of Software Certification	X		
ERDS 0004 - Approval of Computer Security Auditor Employee(s) Attachment A		X	
ERDS 0005 - Application Attachment Vendor Employee(s) and/or Business Entity(ies) Attachment A	X		
ERDS 0006 - Request for Replacement of Certificate or Application Documents	X	X	X
ERDS 0008 - Change of Secure and/or Authorized Access			X
ERDS 0009 - Vendor Application Form for Reference(s) Attachment B	X		
ERDS 0010 - Application for Withdrawal	X	X	X
ERDS 0011 - Secure and Authorized Access Statement			X
BCII 8016 - Request for Live Scan Service	X	X	X
FD-258 - Fingerprint Hard Card	X	X	X

STATE OF CALIFORNIA
Electronic Recording Delivery System (ERDS)
Application for Vendor of Software Certification
ERDS 0003
(orig. 12/05)

DEPARTMENT OF JUSTICE
Division of California Justice Information Services
CJIS Operation Support Bureau
Electronic Recording Delivery System Program

Electronic Recording Delivery System
Application for Vendor of Software Certification

TYPE OR PRINT (IN INK) ALL INFORMATION REQUESTED ON THE APPLICATION.

DOJ USE ONLY	
Cert #	
Date rec'd	
Response date	
Fees	
Analyst	
Tracking #	
HDC date	
Rev. by	
❑ Approved	❑ Denied

TYPE OF APPLICATION

COMPLETE APPLICATION IS REQUIRED FOR EITHER PROCESS.

(CHECK ONE BOX ONLY)

INITITAL ☐ ***RENEWAL*** ☐

The initial and renewal fee(s) is due when submitting this application and is non-refundable. Payment to the Department of Justice (DOJ) must be made by check, cashier's check or money order. No cash will be accepted. For the fee amount applied to this application, reference the Fee Schedule or the California Attorney General Website at http://caag.state.ca.us/erds. If the vendor is requesting certification of employees and/or business entities, the vendor must complete Attachment A and submit proof of fingerprinting BCII 8016 form per each individual listed or a FD-258 fingerprint card with appropriate fingerprinting fees (refer to Fee Schedule and Section 4 of the Vendor of Software Certification handbook).

SECTION A *(APPLICANT INFORMATION - USE ATTACHMENT A FOR MULTIPLE EMPLOYEES AND/OR BUSINESS ENTITIES)*

VENDOR BUSINESS NAME	ERDS CERTIFICATION # *(Required if renewal)*	E-MAIL	
OWNER and/or DESIGNEE	DEALER LICENSE # / STATE		
ADDRESS	CITY	STATE	ZIP CODE
TELEPHONE # ( )	FAX # ( )	SSN	

1. ARE YOU A LEGAL RESIDENT OF CALIFORNIA? ❑ YES ❑ NO IF NO, INCLUDE STATE OF RESIDENCE. _____
2. HAVE YOU EVER USED A NAME OTHER THAN THE ONE ON THIS APPLICATION? ❑ YES ❑ NO IF YES, PLEASE LIST OTHER NAMES BELOW.

   OTHER NAME(S) USED _____
3. HAVE YOU EVER BEEN CONVICTED BY ANY COURT OF A FELONY OR MISDEMEANOR OFFENSE IN CALIFORNIA OR ANY OTHER STATE? ❑ YES ❑ NO IF YES, DISCLOSE THE DATE AND PLACE OF ARREST, WHETHER THE CONVICTION WAS FOR A FELONY OR MISDEMEANOR, AND THE SENTENCE IMPOSED. _____
4. HAVE YOU EVER BEEN ARRESTED IN CALIFORNIA OR ANY OTHER STATE AND/OR ARE YOU AWAITING ADJUDICATION FOR ANY OFFENSE FOR WHICH YOU WERE ARRESTED? ❑ YES ❑ NO IF YES, GIVE DETAILS. (ATTACH ADDITIONAL SHEET AS NEEDED).

SECTION B *(Vendor References)*

EITHER:

A. ON THE APPLICATION ATTACHMENT B, PROVIDE 3 BEST REFERENCES WITHIN THE LAST FIVE YEARS FOR SOFTWARE PRODUCTS OR DEVELOPMENT OF EQUIVALENT TECHNOLOGY, COMPLEXITY, AND SIZE OF AN ELECTRONIC RECORDING DELIVERY SYSTEM. AT LEAST 1 REFERENCE MUST BE FOR A PROJECT USING DOCUMENT IMAGING TECHNOLOGY; **OR**

B. A VENDOR WITH A VALID CALIFORNIA MASTER SERVICES AGREEMENT (CMAS), GENERAL SERVICES AGREEMENT (GSA), OR MASTER SERVICES AGREEMENT (MSA) MUST INCLUDE A COPY OF THIS AGREEMENT IN LIEU OF THE ABOVE REFERENCES, AND A SECRETARY OF STATE CERTIFICATE OF STATUS. THE CMAS, GSA, OR MSA MUST INCLUDE ONE OR MORE OF THE FOLLOWING SERVICE CATEGORIES:

- Consulting-Application Development
- Consulting-IT Acquisition Support
- Consulting-IT Project Management
- Consulting-IT Project Planning
- Consulting-IT Strategic Planning
- Consulting-IT System Implementation
- Consulting-Migration Planning
- Consulting-Software Development
- Consulting-System Analysis
- Consulting-System Design
- Consulting-System Development
- Consulting-System Integration

VENDOR BUSINESS NAME _____

SECTION C *(SOFTWARE APPROVAL)*

I declare under penalty of perjury, as a vendor applying for approval of software, I attest that the software meets the Baseline Requirements and Technology Standards established by the Attorney General (AG) in the areas of imaging standards, transmission and transaction protocols, security, audit/journaling, etc. If any modifications in these areas are made to the software, the certification is invalid. I acknowledge that DOJ's issuance of the approval of the software certificate will include a "disclaimer" stating that the software is not being approved as to its ability to serve/function in an ERDS operational environment nor that it meets all County Recorder's requirements; only that the vendor has stated that it meets the DOJ Baseline Requirements and Technology Standards as of the date of the AG's software approval.

SIGNATURE OF VENDOR: _____
DATE

PRINT NAME: _____

SECTION D *(APPLICATION CHECK LIST)*

CHECK THE BOX IF THESE ITEMS ARE ATTACHED

- ☐ ERDS 0005 ATTACHMENT A *(IF APPLICABLE)*
- ☐ EITHER:
  ERDS 0009 ATTACHMENT B VENDOR REFERENCES; **OR**
  CMAS, GSA, OR MSA AGREEMENT
- ☐ SECRETARY OF STATE CERTIFICATE OF STATUS (IF *APPLICABLE)*
- ☐ PROOF OF FINGERPRINTING (BCII 8016) ; **OR**
  FD-258 FINGERPRINT CARD
- ☐ SSN PRIVACY STATEMENT(S)
- ☐ APPROPRIATE FEE(S)

SECTION E *(TERMS AND CONDITIONS)*

I declare under penalty of perjury under the laws of the State of California that the foregoing information, and all information submitted with this application is true, correct, and complete, and that any false or dishonest answer to any question may be grounds for denial or subsequent termination or suspension of certification. I attest that I have reviewed and agree to the Terms and Conditions of the Vendor Statement and Privacy Statement and I acknowledge that DOJ's issuance of Vendor Certification does not supersede or supplant any of a County Recorder's contracting requirements.

SIGNATURE OF VENDOR: _____
DATE

PRINT NAME: _____

Application Submission

The information on this application and all forms/documentation become the property of the Department of Justice and will be used by authorized personnel to determine the applicant(s) eligibility for certification.

MAIL TO: State of California
Department of Justice
Electronic Recording Delivery System Program
P.O. Box 160526
Sacramento, CA 95816-0526

ERDS Program Contact Information:

Telephone: (916) 227-8907
Fax: (916) 227-0595

E-mail: erds@doj.ca.gov
Website: http://ag.ca.gov/erds

STATE OF CALIFORNIA
Electronic Recording Delivery System
Application Attachment
Vendor Employee(s) and/or Business Entity(ies)
ERDS 0005
(orig. 12/05)

DEPARTMENT OF JUSTICE
Division of California Justice Information Services
CJIS Operation Support Bureau
Electronic Recording Delivery System Program

Electronic Recording Delivery System
APPLICATION ATTACHMENT
VENDOR EMPLOYEE(S) AND/OR BUSINESS ENTITY(IES)

A vendor may apply as an individual or as a company. When applying as a company, the vendor must list on this application form all employees and/or business entity(ies) acting on behalf of the vendor whom will be utilized in the development, installation, testing, maintenance, and/or of having access and/or authorized access to the ERDS. Employees and/or business entity(ies) serving in this capacity are subject to the fingerprint background requirements prior to approval of vendor certification (refer to section [illegible] Vendor of Software Certification Handbook).

ATTACH ADDITIONAL SHEET AS NEEDED

EMPLOYEE REQUESTING ERDS ACCESS

NAME	CLASSIFICATION	DRIVER LICENSE # / STATE	
ADDRESS	CITY	STATE	ZIP CODE
TELEPHONE ( )	FAX ( )		SSN

EMPLOYEE REQUESTING ERDS ACCESS

NAME	CLASSIFICATION	DRIVER LICENSE # / STATE	
ADDRESS	CITY	STATE	ZIP CODE
TELEPHONE ( )	FAX ( )	EMAIL	SSN

EMPLOYEE REQUESTING ERDS ACCESS

NAME	CLASSIFICATION	DRIVER LICENSE # / STATE	
ADDRESS	CITY	STATE	ZIP CODE
TELEPHONE ( )	FAX ( )	EMAIL	SSN

BUSINESS ENTITY ACTING ON BEHALF OF THE VENDOR

BUSINESS NAME	INDIVIDUAL'S NAME	DRIVER LICENSE # / STATE	
ADDRESS	CITY	STATE	ZIP CODE
TELEPHONE ( )	FAX ( )	EMAIL	SSN

I declare under penalty of perjury under the laws of the State of California that the foregoing information and all information submitted with this application is true, correct, and complete, and that any false or dishonest answer to any question may be grounds for denial or subsequent termination or suspension of the vendor's certification.

VENDOR SIGNATURE: _____ DATE

PRINT NAME: _____

BUSINESS NAME: _____

STATE OF CALIFORNIA
Electronic Recording Delivery System (ERDS)
Vendor Application Form for Reference(s)
ERDS 0009
(orig. 12/05)

DEPARTMENT OF JUSTICE
Division of California Justice Information Services
CJIS Operation Support Bureau
Electronic Recording Delivery System Program
Telephone: (916) 227-8907
E-mail: erds@doj.ca.gov

Electronic Recording Delivery System
Vendor Application Form for Reference(s)

TYPE OR PRINT (IN INK) ALL INFORMATION REQUESTED ON THE FORM

INSTRUCTIONS :

This form should be completed and attached to the Application Form # ERDS 0003, if the applicant is providing three best references within the last five years for software products or development of equivalent technology, complexity, and size of an electronic recording delivery system in lieu of providing a copy of a valid agreement (refer to Section 5 of the Vendor of Software Certification Handbook). At least one reference must be for a project using document imaging technology.

APPLICANT NAME

REFERENCE # 1

REFERENCE COMPANY NAME	CONTACT NAME	TELEPHONE # ( )

ADDRESS	CITY	STATE	ZIP CODE

PROJECT NAME AND/OR DESCRIPTION

IDENTIFY THE TASKS AND SERVICES COMPLETED TO-DATE THAT HAVE BEEN PROVIDED/PERFORMED ON THE PROJECT:

(ATTACH ADDITIONAL SHEET AS NEEDED)

REFERENCE # 2

REFERENCE COMPANY NAME	CONTACT NAME	TELEPHONE # ( )

ADDRESS	CITY	STATE	ZIP CODE

PROJECT NAME AND/OR DESCRIPTION

IDENTIFY THE TASKS AND SERVICES COMPLETED TO-DATE THAT HAVE BEEN PROVIDED/PERFORMED ON THE PROJECT:

(ATTACH ADDITIONAL SHEET AS NEEDED)

REFERENCE # 3

REFERENCE COMPANY NAME	CONTACT NAME	TELEPHONE # ( )

ADDRESS	CITY	STATE	ZIP CODE

PROJECT NAME AND/OR DESCRIPTION

IDENTIFY THE TASKS AND SERVICES COMPLETED TO-DATE THAT HAVE BEEN PROVIDED/PERFORMED ON THE PROJECT:

(ATTACH ADDITIONAL SHEET AS NEEDED)

STATE OF CALIFORNIA

Electronic Recording Delivery System (ERDS)
Request for Replacement of Certificate or
Application Documents

ERDS 0006
(orig. 12/05)

DEPARTMENT OF JUSTICE
Division of California Justice Information Services
CJIS Operation Support Bureau
Electronic Recording Delivery System Program

DOJ USE ONLY	
Cert #	
Date rec'd	
Response date	
Fees	
Analyst	
Comments	
Attachment	
Tracking #	
☐ Approved ☐ Denied	

Electronic Recording Delivery System Request for Replacement of Certificate or Application Documents

TYPE OR PRINT (IN INK) ALL INFORMATION REQUESTED ON THE FORM

INSTRUCTIONS:

- To obtain a replacement certificate, complete the Certificate Replacement section of this form and submit the form along with appropriate fees (refer to the Fee Schedule).
- If you are the ERDS certificate holder, you may request copies of your records. Complete the appropriate section of the form and submit the form along with appropriate fees (refer to the Fee Schedule).
- The fee(s) must accompany this form. Faxed copies will not be accepted. The fee must be paid with a check or money order. No cash is accepted.
- Please fill out this form completely and accurately. Incomplete forms will cause a delay in processing your request.
- The requested documents will be mailed to your address designated below.

SECTION A *(Reason for request)*

Please provide certification number: # _____

☐ MY CERTIFICATE WAS LOST, STOLEN, OR DESTROYED
☐ MY CERTIFICATE HAS BEEN MUTILATED TO SUCH AN EXTENT THAT IT IS NO LONGER USABLE.
☐ I DID NOT RECEIVE MY RENEWAL CERTIFICATE IN THE MAIL.
☐ I HAVE CHANGED MY INDIVIDUAL NAME AND/OR ADDRESS AND REQUIRE A NEW CERTIFICATE. (SECTION B MUST BE COMPLETED).
☐ I HEREBY REQUEST THE FOLLOWING APPLICATION DOCUMENTS:
(PLEASE CLARIFY) _____

_____

SECTION B *(Change in Individual Name and/or Address)*

PREVIOUS NAME	CITY	STATE	ZIP CODE
PREVIOUS ADDRESS	TELEPHONE # ( )	FAX # ( )	
NEW NAME	CITY	STATE	ZIP CODE
NEW ADDRESS	TELEPHONE # ( )	FAX # ( )	

I declare under penalty of perjury under the laws of the State of California, that all the information contained herein is true and correct.

SIGNATURE: _____ DATE: _____

PRINT NAME: _____

MAILING ADDRESS: _____

TELEPHONE #: _____ EMAIL: _____

Mail to: Department of Justice
CJIS Operation Support Bureau
Electronic Recording Delivery System
P.O. Box 160526
Sacramento, CA 95816-0526

ERDS Program Contact Information:

Telephone: (916) 227-8907
Fax: (916) 227-0595
E-mail: erds@doj.ca.gov
Website: http://ag.ca.gov/erds

STATE OF CALIFORNIA
Electronic Recording Delivery System (ERDS)
Application for Withdrawal
ERDS 0010
(orig. 12/05)

DEPARTMENT OF JUSTICE
Division of California Justice Information Services
CJIS Operation Support Bureau
Electronic Recording Delivery System Program

Electronic Recording Delivery System Application for Withdrawal

PLEASE REFER TO THE INSTRUCTIONS WHEN COMPLETING THE APPLICATION WITHIN THE APPROPRIATE ERDS HANDBOOK). TYPE OR PRINT (IN INK) ALL INFORMATION REQUESTED.

DOJ USE ONLY	
Cert #	
Date rec'd	
Response date	
Analyst	
HDC Notified	

SECTION A *(WITHDRAWAL INFORMATION)*

CERTIFICATE HOLDER NAME		CERTIFICATE #	
E-MAIL	TELEPHONE # ( )	FAX # ( )	
ADDRESS	CITY	STATE	ZIP CODE
REASON FOR WITHDRAWAL:			

Certificate and Fee Information:

The ERDS Certification is not transferrable and all fees paid are non refundable.

SECTION B *(Declaration)*

I declare under penalty of perjury under the laws of the State of California, that all the information contained herein is true and correct.

SIGNATURE: _____

DATE

PRINT NAME: _____

Application Submission

The information on this application and all forms/documentation become the property of the Department of Justice and will be used by authorized personnel to determine the applicant(s) request for withdrawal.

MAIL TO: State of California
Department of Justice
Electronic Recording Delivery System Program
P.O. Box 160526
Sacramento, CA 95816-0526

ERDS Program Contact Information:

Telephone: (916) 227-8907
Fax: (916) 227-0595
E-mail: erds@doj.ca.gov
Website: http://ag.ca.gov/erds

Fingerprinting Requirements Document

Individual/Role	Fingerprints Required Yes	Fingerprints Required No	Document Referenced
Authorized Submitter			
Upon Secure Access designation by a County Recorder	X		Vendor of Software Certification Handbook
Upon Authorized Access designation by a County Recorder		X	Vendor of Software Certification Handbook
Authorized Access			
Upon Authorized Access designation by a County Recorder		X	Vendor of Software Certification Handbook
Secure Access			
Upon Secure Access designation by a County Recorder	X		*Vendor of Software Certification Handbook*
Vendor of Software			
Upon applying for DOJ Vendor Certification	X		Vendor of Software Certification Handbook
Upon Secure Access designation by a County Recorder if DOJ Vendor Certification is valid		X	Vendor of Software Certification Handbook
Employee of Vendor of Software			
Upon Vendor application for DOJ Vendor Certification	X		Vendor of Software Certification Handbook
Upon Secure Access designation by a County Recorder if DOJ Vendor Certification is valid		X	Vendor of Software Certification Handbook
Business Entity of Vendor of Software			
Upon Vendor application for DOJ Vendor Certification	X		Vendor of Software Certification Handbook
Upon Secure Access designation by a County Recorder if DOJ Vendor Certification is valid		X	Vendor of Software Certification Handbook
County Recorder			
Upon application for DOJ System Certification		X	System Certification Handbook
Change in County Recorder	X		System Certification Handbook
Employee of County Recorder			
Upon Secure Access designation by a County Recorder	X		GC 27393 & 27395
Business Entity of County Recorder			
Upon Secure Access designation by a County Recorder	X		GC 27393 & 27395
Computer Security Auditor			
Upon application for DOJ Auditor Certification	X		Computer Security Auditor Approval Handbook
Upon Secure Access designation by a County Recorder if DOJ Vendor Certification is valid		X	Computer Security Auditor Approval Handbook

State of California

Department of Justice

REQUEST FOR EXEMPTION FROM MANDATORY ELECTRONIC FINGERPRINT SUBMISSION REQUIREMENT

BCII 9004 (3/05)

SAMPLE

Bureau of Criminal Identification and Information
P.O. Box 903417
Sacramento, CA 94203-4170

APPLICANT INSTRUCTIONS: Please type or print clearly all information. Illegible or incomplete information may result in processing delays or denial of your request. Mail this form, together with your fingerprint card(s) (FD258), to the above address.

APPLICANT'S NAME: _____
LAST FIRST MIDDLE

APPLICANT'S ADDRESS:

_____
STREET CITY COUNTY STATE ZIP CODE

EMPLOYER OR LICENSING AGENCY:

_____

BASIS FOR EXEMPTION:

1. NO REGIONAL ACCESS TO FINGERPRINTING SERVICES:

   Nearest Electronic Fingerprint Site: (Refer to public sites listed on the Attorney General's website at http://ag.ca.gov/fingerprints/publications/contact.htm)

   _____
   BUSINESS NAME ADDRESS

2. OTHER (explain): _____

   _____

   _____

Pursuant to California Penal Code section 11077.1(b), I request an exemption from the mandatory electronic fingerprint submission requirement. I certify that the foregoing is true and correct.

_____ _____
APPLICANT'S SIGNATURE DATE

The Department of Justice will evaluate your request and determine whether adequate justification exists to accept your hard fingerprint card(s) in order to process a request for criminal offender record information for employment, licensing, certification, child placement, or adoption purposes.

REQUEST FOR LIVE SCAN SERVICE SAMPLE

Applicant Submission

ORI: CA0349400 (Code assigned by DOJ) Type of Application: ERDS SEC ACCESS GC 27895

Job Title or Type of License, Certification or Permit: ERDS SECURE ACCESS

Agency Address Set Contributing Agency:

Department of Justice — Agency authorized to receive criminal history information

09956 — Mail Code (five digit code assigned by DOJ)

4949 Broadway — Street No.Street or P.O. Box

ERDS Program — Contact Name (Mandatory for all school submissions)

Sacramento (City) CA (State) 95820 (Zip Code)

(916) 227-8907 — Contact Telephone No.

Name of Applicant: (please print) Last First MI

Alias: Last First

Driver's License No.

Date of Birth: Sex: ☐ Male ☐ Female

Misc. No. **BIL-** Agency Billing Number (if applicable)

Height: Weight: Misc. No:

Eye Color: Hair Color: Home Address: Street or P.O. Box

Place of Birth: City, State and Zip Code

SOC:

Your Number: OCA No. (Agency Identifying No.)

Level of Service DOJ [X] FBI [X]

If resubmission, list Original ATI No.

Employer: (Additional response for agencies specified by statute)

Employer Name

Street No. Street or P.O. Box

Mail Code (five digit code assigned by DOJ)

City State Zip Code

( ) Agency Telephone No. (optional)

Live Scan Transaction Completed By: Name of Operator Date:

Transmitting Agency ATI No. Amount Collected/Billed

BCII 8016 (Rev 04/01) ORIGINAL – Live Scan Operator, SECOND COPY – Requesting Agency, THIRD COPY - Applicant

APPLICANT

LEAVE BLANK

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM | FIRST NAME | MIDDLE NAME

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED

ALIASES AKA

RESIDENCE OF PERSON FINGERPRINTED

CA0349400
BU OF ID & INFO
SACRAMENTO CA

DATE OF BIRTH DOB
Month Day Year

CITIZENSHIP

SEX	RACE	HGT	WGT	EYES	HAIR	PLACE OF BIRTH POB

DATE

SIGNATURE OF OFFICIAL TAKING FINGERPRINTS

YOUR NO. OCA

EMPLOYER AND ADDRESS

FBI NO. FBI

ARMED FORCES NO. MNU

LEAVE BLANK

CLASS

REASON FINGERPRINTED

SOCIAL SECURITY NO. SOC

REF.

MISCELLANEOUS NO. MNU

Sample

1. R. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING	5. R. LITTLE
6. L. THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING	10. L. LITTLE

LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY | L. THUMB | R. THUMB | RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY